

[E-Commerce Times](#) > [Industries](#) > [Healthcare](#) | [Read Next Article in Healthcare](#)

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at (818) 461-9700 or visit <http://www.ectnews.com/about/reprints/>.

HIPAA Revisited, Part 1: Privacy vs. Portability



By Andrew Burger
[CRM Buyer](#)
 Part of the ECT News Network
 05/24/08 4:00 AM PT

 [Print Version](#)
 [E-Mail Article](#)
 [Digg It](#)
 [Reprints](#)

In the 12 years since the Health Insurance Portability and Accountability Act was enacted, organizations have gone to great lengths to comply. However, advances in technology are leading to calls for more flexibility in the movement of personal health information.


Responding to heightened concerns about the privacy of individuals' medical and healthcare information, the federal government in 1996 introduced HIPAA, the Health Insurance Portability and Accountability Act. It empowered the Department of Health and Human Services to develop and manage the methods governing the collection and sharing of personal health information and the mechanisms with which all U.S. healthcare organizations covered under the Act must comply.

So-called covered entities needed to be in compliance with the provisions of the Act by April 14, 2003. As is the nature of introducing new and sweeping changes throughout a huge industry, HIPAA has had unexpected consequences, imposed additional administrative and financial burdens on healthcare organizations of all shapes and sizes, generated misconceptions, and provoked its share of criticism.

Is HIPAA proving effective in protecting the privacy of individuals' personally identifiable health information? And are the resulting accounting and reporting systems proving manageable for the diversity of healthcare practitioners and administrators? Is it getting in the way of medical treatment and research or facilitating it? CRM Buyer spoke with a range of people who, from various perspectives, have had to come to grips with HIPAA and its implications.

Health, Democracy and Technology

In March, the [Center for Democracy and Technology](#) joined forces with the [Health Privacy Project](#) and announced the launch of an ambitious project on health privacy and [information technology](#). Led by Janlori Goldman, a nationally recognized leader in the field, the Health Privacy Project for the past 10 years has been at the forefront of independent public policy research as it relates to privacy, medical and healthcare information.

The CDT's Health Privacy Project on May 15 released its first policy paper, which urges "policymakers and the private sector to develop and implement a comprehensive privacy and [security](#)  framework to govern the wide range of computer and Internet-based systems being created to share sensitive health

information."

Despite HIPAA, the push for more fungible and liquid health information is on, according to the CDT, justified by members of the medical and IT industries. They claim that medical and health data needs to flow freely if advances in research and development, as well as treatment, are to be realized.

"This is a critical time for health information privacy. Technologies are being deployed and systems are being designed that will have a far-reaching impact on how personal health information is accessed, stored and shared," according to Deven McGraw, Goldman's successor as director of the Health Privacy Project, now under the auspices of the CDT.

"Consumers want the benefits of HIT (Health Information Technology)-enabled healthcare and they want assurances that their privacy will be protected," McGraw said. "We can and must move forward on both fronts."

Post-HIPAA Operative Action Needed

"We believe policymakers need to take a long-term approach to these issues," McGraw told CRM Buyer. "CDT is urging Congress to hold hearings on a broad range of privacy and security issues in health IT, and we plan to informally gather together a group of diverse health IT stakeholders over the next several months to identify the issues that need to be addressed and possibly come up with some consensus solutions.

"At the same time, we are supporting some incremental steps that Congress can include in legislative proposals that are pending now that will move the ball forward in securing greater privacy and security protections for electronic personal health information."

These concerns would best be addressed by a comprehensive national privacy and security framework based on fair information practices, such as those set forth in the Markle Foundation's Connecting for Health Common Framework, to govern personal health information in the new e-health environment, McGraw explained.

"This framework needs to be adopted by all stakeholders -- policymakers need to look at how to address the framework in law, and the organizations handling the information need to incorporate a framework in business ☞ 'best practices.'"

HIPAA in Practice

HIPAA created a significant burden for many healthcare providers and others covered by the rules if it was implemented thoroughly, according to Kirk J. Nahra, attorney and privacy specialist at Washington D.C.'s Wiley, Rein LLP.

"But most of this burden involved initial compliance with the rule, primarily developing and implementing appropriate policies and procedures for compliance. Once that significant initial burden was undertaken, ongoing compliance is primarily an issue of staying abreast of developments and filling any gaps that develop."

While there was a lot of concern that HIPAA might have negative effects and consequences for patient care, Nahra added that he is not aware of any significant evidence that this has proven to be the case.

"Most healthcare providers, particularly hospitals and other large organizations, have done a reasonable and thorough job on HIPAA compliance. There are pockets of providers who have done less, especially small physician practices, but there is little evidence that this reduced effort has had any particular adverse impact because those physicians are not the kinds of people that are trying to push the envelope on what can be done with patient information," he commented.

HIPAA at College Park

Operating a university healthcare center and with a wide range of medical and healthcare research programs in progress, the University of Maryland at College Park is considered a "hybrid entity" under HIPAA. In other words, it is one where some of its constituent organizations and activities making use of and sharing PHI (personal health information) as defined by the Act are considered "covered entities" subject to HIPAA's provisions while others, such as some of its research programs, are not.

The University Health Care Center has been fully compliant with HIPAA since the implementation of its Privacy Act in 2003 and Security Act in 2005, Deirdre A. Younger, assistant director for IT and operations, told CRM Buyer.

"HIPAA has not proven to be burdensome or a barrier to providing patient care. The UHC has always upheld the highest level of privacy for patients and their information; this was true even prior to the implementation of HIPAA."

Healthcare information has always been bound by confidentiality rules and regulations, Younger noted.

"HIPAA elaborated on how to better protect PHI, required that policies and procedures be developed -- if not already developed -- and that patients be provided with written notice of an organization's privacy practices. The most noticeable change since implementation has been to ensure that patients receive and acknowledge their receipt of our Notice of Privacy Practices."

Complying with the HIPAA Security Act has required the University Health Center's IT department to be constantly diligent in maintaining the security of electronic patient data. In conformance with the Act's provisions, the IT department has installed the required [firewalls](#) to enhance and ensure security.

UHC's compliance efforts also included staff training and education. "We work to continuously ensure the privacy and security of all patient information. We provided all employees with HIPAA training prior to its implementation and all new employees are trained on their first day of employment at the UHC," Younger added. **ECT**

Stay tuned for Part 2 of this two-part series.

[Click here](#) to be notified when the next installment in this series is published.

Social Networking Toolbox: [ShareThis](#)

Next Article in Healthcare: [Google Offers Virtual Filing Cabinet for Health Records](#)



Copyright 1998-2008 ECT News Network, Inc. All Rights Reserved. See [Terms of Service](#) and [Privacy Policy](#). [How To Advertise](#).